Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
Implementation of the Telecommunications	)	
Act of 1996: Telecommunications Carriers'	)	
Use of Customer Proprietary Network	)	CC Docket No. 96-115
Information and Other Customer Information	)	
	)	
Comments Sought on Privacy and Security	)	
of Information Stored on Mobile	)	
Communications Devices	)	

COMMENTS OF THE FUTURE OF PRIVACY FORUM

The Future of Privacy Forum ("FPF") submits these comments in response to the May 25, 2012 Public Notice in the above-captioned proceeding,[1] which seeks comment on "the privacy and data security practices of mobile wireless service providers with respect to customer information stored on their users' mobile communications devices, and the application of existing privacy and security requirements to that information."[2] As discussed below, the mobile wireless marketplace has changed dramatically in recent years, producing intense competition for mobile data services (including mobile device applications, or "apps") and an extremely decentralized data collection and use environment. The Federal Communications Commission ("Commission") should recognize this newly diverse paradigm and the need to address mobile data privacy and security concerns via efforts that are able to engage this broad ecosystem. It should also work with all stakeholders to educate consumers better about the myriad tools available to protect their personal information that is stored on mobile devices.

[1] *Comments Sought on Privacy and Security of Information Stored on Mobile Communications Devices*, CC Docket No. 96-115, Public Notice, DA 12-818 (WCB WTB OGC rel. May 25, 2012) ("*Notice*").

[2] *Id.* at 1.

I. ABOUT THE FUTURE OF PRIVACY FORUM AND ITS EFFORTS TO DEVELOP IMPROVED MOBILE PRIVACY AND DATA SECURITY PRACTICES

FPF is a Washington, DC-based think tank focused on advancing responsible data practices. FPF is led by privacy leaders Jules Polonetsky and Christopher Wolf and includes an advisory board comprised of leading figures from industry, academia, law and advocacy groups.[3] FPF seeks to advance meaningful self-regulation and best practices for consumer privacy and has significant experience in working with stakeholders to address mobile privacy issues.

FPF has actively worked to focus attention on the data collection issues raised by mobile apps and other mobile services. To further this effort, FPF created a resource center at www.applicationprivacy.org that contains privacy guidelines, platform and application store requirements, privacy policy generators, and self-assessment tools, as well as relevant laws and regulatory guidance, all of which can assist app developers and other members of the mobile wireless ecosystem in providing their users with appropriate privacy protections. FPF also recently released the *Best Practices for Mobile Application Developers*,[4] created jointly with the Center for Democracy and Technology.

FPF also regularly conducts surveys of app privacy policies.[5] In the latest survey released on July 11, 2012, FPF reviewed the most popular paid and free apps on leading app

[3] The positions taken by FPF are entirely its own and do not necessarily reflect those of its supporters and advisory board members.

[4] *Best Practices for Mobile Application Developers*, Future of Privacy Forum and Center for Democracy & Technology, *available at* http://www.futureofprivacy.org/best-practices-for-mobile-app-developers/.

[5] *Future of Privacy Forum Study Results Show App Developers Heed Call for Privacy Policies*, Press Release, Future of Privacy Forum (July 11, 2012), *available at* http://www.futureofprivacy.org/2012/07/11/fpf-study-results-show-app-developers-heed-call-for-privacy-policies/ ("July 2012 Survey Press Release"); *FPF Survey: Free Apps Better than Paid on Privacy Policies*, Press Release, Future of Privacy Forum (Dec. 20, 2011), *available at* http://www.futureofprivacy.org/wp-content/uploads/FPF-Mobile-Apps-release.pdf.

platforms, documenting which ones provided consumers with a privacy policy describing the apps' data collection and use practices.[6] The study found that the percentage of apps with privacy policies has grown rapidly since the previously FPF study conducted in September 2011, and that almost all leading apps that collection precise location information now provide a privacy policy.[7] In addition, on April 25, 2012, FPF co-hosted a day-long App Developer Privacy Summit (along with the Application Developers Alliance and the Stanford Center for Information and Society), which attracted hundreds of app developers and other attendees to discuss privacy and data security concerns.[8] FPF's firsthand experience demonstrates that collective action involving a broad range of industry players, privacy and consumer groups, academics, and technical experts is the optimal way to make real progress in enhancing consumer privacy and data security.

II. THE MOBILE WIRELESS ECOSYSTEM HAS CHANGED DRAMATICALLY IN RECENT YEARS, PRODUCING INTENSE COMPETITION FOR MOBILE APPS AND OTHER DATA SERVICES.

In the *Notice*, the Commission seeks comment regarding how the practices of mobile wireless service providers have evolved since 2007 with respect to information stored on their customers' mobile communications devices.[9]

As the *Notice* recognizes, the mobile wireless ecosystem has "evolved dramatically" in the last few years.[10] Five years ago, Apple introduced the iPhone. The Apple App store and the Android Market did not appear until 2008. And it was not until 2010 that the tablet market

[6] July 2012 Survey Press Release.

[7] *Id.*

[8] *See App Developer Privacy Summit*, http://cyberlaw.stanford.edu/events/app-developer-privacy-summit.

[9] *Notice* at 4.

[10] *Id.* at 1.

began to take off. Today, mobile devices – once limited to basic communications functions, can now provide an array of integrated functions that previously were handled by dozens of separate consumer electronics products. The majority of mobile subscribers now have smartphones, and smartphone sales are exceeding personal computer ("PC") sales.[11] Tablet sales are also expected to outpace PC sales within a few years.[12] In addition, mobile apps have also quickly become a part of everyday life for many Americans, with more than a million apps now available. In fact, the mobile app economy – less than three years old – is now estimated to support a half million jobs.[13] This unprecedented growth has revolutionized how mobile services are delivered and created an array of choices and intense competition for every type of service delivered over a mobile device.

These changes have also brought an accompanying paradigm shift in both the role of wireless carriers in providing mobile data services *and* the collection and use of personal information stored on mobile devices. Several years ago, regulated wireless carriers provided network services, sold devices directly to consumers, and typically decided what apps could be made available for each wireless device (with some using an integrated "walled garden" approach). Under this highly integrated model, carriers were the focal point for such collection and use.

Today, the mobile smartphone environment is an open, dynamic, chaotic system of highly competitive platforms and services, which has "revolutionized the ability to generate,

---

[11] *See* Prepared Remarks of FCC Chairman Julius Genachowski, International CTIA Wireless 2012, New Orleans, 2 (May 8, 2012).

[12] *Id.*

[13] *Id.*

communicate, share, and access data."[14] Data has become "the raw material of production, a new source of immense economic and social value" that "create[s] enormous value for the global economy, driving innovation, productivity, efficiency, and growth."[15] Dozens of companies have a role in providing innovative new features and services to consumers, and each collects and uses data obtained from mobile devices in various ways. For example, the list below contains some of the key participants in today's mobile wireless ecosystem:

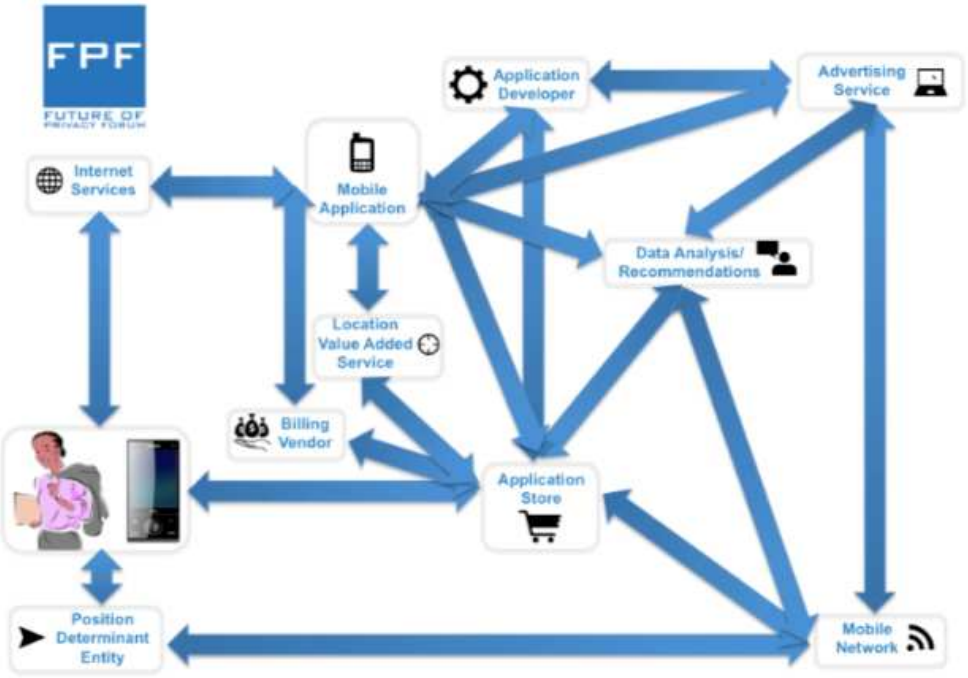
- Mobile Handset and Tablet Manufacturers;
- Other Original Equipment Manufacturers ("OEMs");
- Router Manufacturers;
- Mobile Device Chip Providers;
- Mobile Operating System Providers;
- Mobile Web Browser Developers;
- App Store and Platform Operators;
- Mobile App Developers;
- Third-Party Data Aggregators;
- Mobile Advertising Networks;
- Position Determinant Vendors;
- Location Value-Added Service Providers;
- Near-Field Communications Applications Providers;
- Mobile Video Software Developers;
- Mobile Packet Core Network Operators;
- Mobile Semiconductor Operators;
- SMS/MMS Messaging Service Providers;
- Mobile Satellite Operators; and
- Mobile Site and Mobile App Analytics Providers.

---

[14] Omar Tene and Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 Stan. L. Rev. Online 63 (Feb. 2, 2012), *available at* http://www.stanfordlawreview.org/online/privacy-paradox/big-data.

[15] *Id.*

The diagram below highlights further the complex exchange of information occurring in the mobile wireless ecosystem.



III. THE COMMISSION SHOULD RECOGNIZE THAT MOBILE DATA PRIVACY AND SECURITY CONCERNS NEED TO BE ADDRESSED ACROSS THE DIVERSE MOBILE WIRELESS ECOSYSTEM.

The Commission should recognize the newly diverse paradigm for mobile data services.[16] Importantly, carriers today represent just one segment of this highly decentralized network of transactions, and the vast majority of the data that is stored or obtained from mobile devices today is not customer proprietary network information ("CPNI").[17] The Commission therefore should avoid focusing on carriers as a sole "touch point" for addressing mobile data privacy and

[16] *See Notice* at 4-5 (seeking comment on carriers' obligations under Section 222).

[17] CPNI is defined as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." 47 U.S.C. § 222(h)(1).

security concerns in light of the number of interrelated parties that comprise the mobile wireless ecosystem.

The Commission's complex CPNI model was initially created for legacy voice telephone services and stems from a pre-broadband era of heavy-handed structural and economic regulation that is inappropriate for today's competitive marketplace. Today, mobile apps that provide Voice over Internet Protocol ("VoIP") services (including non-interconnected VOIP services) and phone-to-phone messaging features compete directly with traditional wireless carrier voice and text messaging plans. Moreover, new "integrated" broadband voice, messaging, and data service platforms have emerged in the last few years, attempting to replace traditional, carrier-provided wireline and wireless services. Many of these new apps, services, and platforms (some of which are advertising-supported) are not "telecommunications services" or "interconnected VoIP services" and therefore are free of the Commission's rigid CPNI requirements.

In addition, the Federal Trade Commission ("FTC"), the National Telecommunications & Information Administration ("NTIA"), and state attorneys general are already fully engaged with the principal players in the mobile wireless ecosystem to address mobile privacy and data security concerns. Specifically, the FTC's comprehensive Privacy Report released earlier this year recommended that companies providing mobile services improve their privacy practices, including through the use of shorter, more meaningful disclosures.[18] FTC staff has also initiated a project to update the FTC's guidance about online advertising disclosures, and the FTC held a workshop on May 30, 2012 to address, *inter alia*, mobile privacy disclosures.[19] This week,

[18] *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, FTC Report, 13-14 (Mar. 2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

[19] In Short: Advertising & Privacy Disclosures in a Digital World, Federal Trade Commission Workshop (May 30, 2012), *at* http://ftc.gov/bcp/workshops/inshort/index.shtml.

NTIA convened a multistakeholder effort intended to develop a voluntary, enforceable code of conduct for mobile application transparency.[20] In February 2012, the California Attorney General entered into a Joint Statement of Principles agreement with six major app store platforms, setting forth requirements related to app privacy.[21] Recently, Facebook also joined this agreement and is now requiring that all apps in its App Center have privacy policies.[22] In addition, FPF is a member of the group convened by the California State Director of Privacy that is working to create best practices for app developers. These extensive efforts – involving stakeholders from multiple segments of the mobile wireless ecosystem – illustrate further why contemporary mobile data privacy and security concerns need to be addressed on an ecosystem-wide basis.

IV. THE COMMISSION SHOULD WORK WITH STAKEHOLDERS TO EDUCATE CONSUMERS AND APP DEVELOPERS ABOUT THE IMPORTANCE OF PROTECTING THE PRIVACY AND SECURITY OF INFORMATION STORED ON MOBILE DEVICES.

The privacy and security of user data is an important issue for the entire mobile wireless ecosystem. Users must trust mobile devices, apps, and services with their data or they will be more hesitant to download and use the services – jeopardizing the entire mobile data economy. And all companies need to remember that accessing user data is a privilege, not a right.

---

[20] July 12, 2012 Privacy Multistakeholder Meeting: Details, National Telecommunications & Information Administration (June 26, 2012), *at* http://www.ntia.doc.gov/other-publication/2012/july-12-2012-privacy-multistakeholder-meeting-details ("The objectives of the July 12, 2012 meeting are to: 1) promote discussion among stakeholders concerning mobile app transparency by employing a structured, open process; and 2) provide a venue for stakeholders to agree on the schedule and format of future meetings.").

[21] *See Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications*, Press Release, California Department of Justice Office of the Attorney General (Feb. 22, 2012), *available at* http://oag.ca.gov/news/press_release?id=2630.

[22] *Facebook to require privacy policies for all apps in App Center*, Los Angeles Times (June 22, 2012), *available at* http://articles.latimes.com/2012/jun/22/business/la-fi-facebook-ag-20120622.

The Commission should continue to encourage stakeholders to protect the privacy and security of personal information, including information that is stored on mobile devices. In particular, it should help stakeholders educate consumers about the importance of protecting their personal information. For example, the Commission should develop a web page with tips for protecting information stored on mobile devices. The page could also include information regarding (and links to) independent publications or websites that describe and review the helpful privacy-enhancing apps and other tools that are available to consumers. Through these efforts, the Commission can help empower consumers with respect to their personal information.

The Commission should also encourage companies that enable and support mobile apps to ensure that app developers have access to essential privacy information and tools, including the resources needed to create privacy policies. For example, a number of companies such as AT&T, Facebook, and Sprint point app developers for their platforms to the FPF resource site at www.applicationprivacy.org. In addition, the Commission should support and promote ongoing industry advances in transparency and consumer choice. For example, the Commission could encourage carriers and other stakeholders to participate in NTIA's ongoing multistakeholder process. Moreover, as part of its education efforts, the Commission could develop an industry-focused web page with links to privacy resources and tools for carriers and app developers, such as those from FPF, CTIA, PrivacyChoice, TRUSTe, and others.

Finally, the Commission should support efforts by carriers to provide meaningful transparency and consumer choice with respect to their information practices for mobile devices, and should encourage innovation with respect to how such goals are accomplished.

Respectfully submitted,

/s/ Jules Polonetsky

_____

Jules Polonetsky

Co-Chair and Director
Future of Privacy Forum
919 18th Street, NW Suite 901
Washington, DC 20006
(202) 713-9466
julespol@futureofprivacy.org

Christopher Wolf
Founder and Co-Chair
Future of Privacy Forum

Partner
Hogan Lovells US LLP
555 13th Street, NW
Washington, DC 20004
(202) 637-8834
christopher.wolf@hoganlovells.com

Counsel for the
Future of Privacy Forum

July 13, 2012